

GIBSON, DUNN & CRUTCHER LLP  
S. ASHLIE BERINGER, SBN 263977  
ABeringer@gibsondunn.com  
JOSHUA JESSEN, SBN 222831  
JJessen@gibsondunn.com  
JEANA BISNAR MAUTE, SBN 290573  
JBisnarMaute@gibsondunn.com  
JESSICA S. OU, SBN 280534  
JOu@gibsondunn.com  
1881 Page Mill Road  
Palo Alto, California 94304  
Telephone: 650.849.5300  
Facsimile: 650.849.5333

GIBSON, DUNN & CRUTCHER LLP  
GAIL E. LEES, SBN 90363  
GLEes@gibsondunn.com  
333 South Grand Avenue  
Los Angeles, California 90071  
Telephone: 213.229.7000  
Facsimile: 213.229.7520

Attorneys for Defendant  
APPLE INC., A CALIFORNIA CORPORATION

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

In re iPhone Application Litigation

CASE NO. 11-MD-02250-LHK

**CLASS ACTION**

**DEFENDANT APPLE INC.'S  
OPPOSITION TO PLAINTIFFS' MOTION  
FOR CLASS CERTIFICATION**

**HEARING:**

Date: October 31, 2013  
Time: 1:30 p.m.  
Place: Courtroom 4  
Judge: The Honorable Lucy H. Koh

**PROPOSED REDACTED COPY**

## TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION .....	1
II. FACTUAL BACKGROUND—IDEVICE CLAIMS .....	2
A. Plaintiffs’ Newly Expanded “iDevice Class” .....	3
B. Named iDevice Plaintiffs .....	3
C. Alleged Misrepresentations and Omissions .....	4
1. UDID as “Non-Personal Information” .....	5
2. Promise to Use SSL Encryption on Apple Web Pages .....	6
D. Plaintiffs’ New Critiques of Apple’s Business and Technology .....	6
1. “Uneven Enforcement” of the PLA and App Review Guidelines .....	6
2. Complaints About Device Resource Depletion .....	8
E. The Proposed Injunctive Relief Was Mooted by iOS Changes Beginning with iOS 5 .....	9
III. FACTUAL BACKGROUND—GEOLOCATION CLAIMS .....	10
A. Plaintiffs’ Previously Proposed “Location Services ‘Off’ Class” and Their Newly Expanded “Geolocation Class” .....	10
1. The Newly Defined Proposed Geolocation Class .....	10
2. Plaintiffs’ Geolocation Allegations .....	10
B. Named Geolocation Plaintiffs .....	11
C. iOS 4 Bug Triggered Rarely and in Highly Fact-Specific Circumstances .....	12
1. No Transmission of “Your Location” Data .....	12
2. No Impact on Location Services Setting .....	12
D. Plaintiffs’ Newly Invented Geo-tagging Theory (Based on Pre-iOS 4.1) .....	13
IV. NO CLASS CAN BE CERTIFIED BECAUSE PLAINTIFFS LACK STANDING .....	13
V. THE PROPOSED CLASSES ARE OVERBROAD AND NOT ASCERTAINABLE .....	15
VI. PLAINTIFFS CANNOT CERTIFY A CLASS BASED ON UNALLEGED THEORIES .....	16
VII. PLAINTIFFS CANNOT SATISFY THE REQUIREMENTS OF RULE 23(A) .....	17

1	A.	The Named Plaintiffs—Who Suffered No Injury, Had No Data Transmitted, Are Not Concerned by and Continue to Engage in the Challenged Practices—Are Not Typical .....	17
2			
3	B.	Plaintiffs Have Not Satisfied, and Cannot Satisfy, the Commonality Requirement .....	19
4			
5	1.	Plaintiffs Do Not Meet Their Burden of Demonstrating Common Evidence .....	19
6	2.	Plaintiffs’ UCL “Fraud” Claims Are Highly Individualized .....	19
7	a.	Location Services Provisions: SLA and Device Setting .....	20
8	b.	Privacy Policy Definition of UDID as “Non-Personal Information” .....	20
9	c.	SSL Encryption Claim .....	21
10	3.	Plaintiffs’ UCL “Unfairness” Claims Are Highly Individualized .....	21
11	a.	Supposed “Uneven Enforcement” Of App Review Guidelines .....	22
12	b.	Resource Consumption As A Result of “Unauthorized Transmissions” Depends on Myriad Factors .....	23
13			
14	4.	Plaintiffs’ CLRA Claims Require Individualized Determinations of Damage and Reliance That Preclude Commonality .....	23
15			
16	C.	Plaintiffs Have Not Satisfied, and Cannot Satisfy, the Adequacy Requirement .....	24
17	VIII.	THE PUTATIVE CLASSES CANNOT BE CERTIFIED UNDER RULE 23(B)(2) .....	25
18	A.	Plaintiffs Fail to Cite Any Ongoing or Imminent Harm That Could Be Redressed .....	25
19	B.	The Proposed Relief Would Not Benefit the Class as a Whole—or Even Most of It .....	26
20			
21	IX.	THE PUTATIVE “LIABILITY-ONLY” CLASS (“BATTERY LIFE/BANDWIDTH CLASS”) CANNOT BE CERTIFIED UNDER RULE 23(B)(3) .....	27
22	X.	CONCLUSION .....	28

## TABLE OF AUTHORITIES

Page(s)**Cases**

<i>Aberdeen v. Toyota Motor Sales, U.S.A.,</i> No. CV-08-1690-PSG, 2009 WL 7715964 (C.D. Cal. June 23, 2009), <i>aff'd in</i> <i>relevant part</i> , 422 F. App'x 617 (9th Cir. 2011).....	18
<i>Allied Orthopedic Appliances, Inc. v. Tyco Healthcare Grp. L.P.,</i> 247 F.R.D. 156 (C.D. Cal. 2007) .....	25
<i>Amchem Prods., Inc. v. Windsor,</i> 521 U.S. 591 (1997) .....	28
<i>Arnold v. United Artists Theatre Circuit, Inc.,</i> 158 F.R.D. 439 (N.D. Cal. 1994) .....	27
<i>Birdsong v. Apple, Inc.,</i> 590 F.3d 955 (9th Cir. 2009).....	14
<i>Bodner v. Oreck Direct, LLC,</i> No. C 06-4756 MHP, 2007 WL 1223777 (N.D. Cal. Apr. 25, 2007).....	18
<i>Burdick v. Union Sec. Ins. Co.,</i> No. CV 07-4028 ABC (JCX), 2009 WL 6541608 (C.D. Cal. April 2, 2009) .....	27
<i>Campion v. Old Republic Home Prot. Co., Inc.,</i> 272 F.R.D. 517 (S.D. Cal. 2011).....	23
<i>Caro v. Procter &amp; Gamble Co.,</i> 18 Cal. App. 4th 644 (1993) .....	24
<i>Carrera v. Bayer Corp.,</i> No. 12-2621, 2013 U.S. App. LEXIS 17479 (3d Cir. Aug. 21, 2013) .....	15, 16
<i>Chamberlan v. Ford Motor Co.,</i> 369 F. Supp. 2d 1138 (N.D. Cal. 2005) .....	24
<i>Cholakyan v. Mercedes-Benz USA, LLC,</i> 281 F.R.D. 534 (C.D. Cal. Mar. 28, 2012) .....	17, 26, 27
<i>City of Los Angeles v. Lyons,</i> 461 U.S. 95 (1983).....	15, 25
<i>Clapper v. Amnesty Int'l USA,</i> 133 S. Ct. 1138 (2013) .....	14
<i>Clemens v. DaimlerChrysler Corp.,</i> 534 F.3d 1017 (9th Cir. 2008).....	19
<i>Comcast Corp. v. Behrend,</i> 133 S. Ct. 1426 (2013) .....	1, 28

**TABLE OF AUTHORITIES**  
(continued)

	<u>Page(s)</u>
<i>Davis v. HSBC Bank Nevada, N.A.</i> , 691 F.3d 1152 (9th Cir. 2012).....	22
<i>Deitz v. Comcast Corp.</i> , No. C 06-06352 WHA, 2007 WL 2015440 (N.D. Cal. Jul. 11, 2007) .....	24
<i>Ellis v. Costco Wholesale Corp. (II)</i> , 285 F.R.D. 492, 539 (N.D. Cal. 2012).....	28
<i>Ellis v. Costco Wholesale Corp.</i> , 657 F.3d 970 (9th Cir. 2011).....	17, 21, 25
<i>Endres v. Wells Fargo Bank</i> , No. C 06-7019 PJH, 2008 WL 344204 (N.D. Cal. Feb. 6, 2008).....	18
<i>Evans v. IAC/Interactive Corp.</i> , 244 F.R.D. 568 (C.D. Cal. 2007) .....	17
<i>Evans v. Linden Research, Inc.</i> , No. C 11-01078 DMR, 2012 WL 5877579 (N.D. Cal. Nov. 20, 2012).....	13
<i>Guido v. L’Oreal, USA, Inc.</i> , CV 11-1067 CAS JCX, 2013 WL 3353857 (C.D. Cal. July 1, 2013) .....	28
<i>Hanni v. Am. Airlines, Inc.</i> , No. C 08–00732 CW, 2010 WL 289297 (N.D. Cal. Jan. 15, 2010) .....	16
<i>Hanon v. Dataproducts Corp.</i> , 976 F.2d 497 (9th Cir. 1992).....	18
<i>In re Actimmune Mktg. Litig.</i> , No. C 08-02376-MHP, 2009 WL 3740648 (N.D. Cal. Nov. 6, 2009).....	22
<i>In re Flash Memory Antitrust Litig.</i> , No. C 07-0086 SBA, 2010 WL 2332081 (N.D. Cal. June 9, 2010) .....	26
<i>In re Google Android Consumer Privacy Litig.</i> , No. 11-MD-02264 JSW, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013) .....	14
<i>In re LinkedIn User Privacy Litig.</i> , No. 12-CV-03088 EJD, 2013 WL 844291 (N.D. Cal. Mar. 6, 2013).....	14
<i>In re New Motor Vehicles Canadian Export Antitrust Litig.</i> , 522 F.3d 6 (1st Cir. 2008).....	26
<i>In re Vioxx Class Cases</i> , 180 Cal. App. 4th 116 (2009) .....	24
<i>In re Wells Fargo Home Mortgage Overtime Pay Litig.</i> , 571 F.3d 953 (9th Cir. 2009).....	28

**TABLE OF AUTHORITIES**  
(continued)

	<u>Page(s)</u>
<i>In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig.</i> , 722 F.3d 838 (6th Cir. 2013).....	28
<i>Jenkins v. Apple Inc.</i> , No. 11-CV-01828-LHK, 2011 U.S. Dist. LEXIS 71261 (N.D. Cal. July 1, 2011) .....	14
<i>Jordan v. Cnty. of Los Angeles</i> , 669 F. 2d 1311 (9th Cir. 1982), <i>vacated on other grounds</i> , 459 U.S. 810 (1982).....	19
<i>Kaldenbach v. Mut. of Omaha Life Ins. Co.</i> , 178 Cal. App. 4th 830 (2009) .....	22
<i>Lierboe v. State Farm Mut. Auto. Ins. Co.</i> , 350 F.3d 1018 (9th Cir. 2003).....	13
<i>Mazur v. eBay, Inc.</i> , 257 F.R.D. 563 (N.D. Cal. 2009).....	15, 16
<i>Mazza v. Am. Honda Motor Co.</i> , 666 F.3d 581 (9th Cir. 2012).....	13, 16, 20, 22
<i>Menagerie Prods. v. Citysearch</i> , No. CV 08-4263 CAS, 2009 U.S. Dist. LEXIS 108768 (C.D. Cal. Nov. 9, 2009) .....	23
<i>Meyer v. Sprint Spectrum L.P.</i> , 45 Cal. 4th 634 (2009) .....	24
<i>Munoz v. PHH Corp.</i> , 1:08-CV-0759-AWI-BAM, 2013 WL 2146925 (E.D. Cal. May 15, 2013) .....	28
<i>Nelsen v. King Cnty.</i> , 895 F.2d 1248 (9th Cir. 1990).....	13
<i>O'Shea v. Littleton</i> , 414 U.S. 488 (1974).....	14, 25
<i>Pecover v. Elec. Arts Inc.</i> , No. C 08-2820 VRW, 2010 WL 8742757 (N.D. Cal. Dec. 21, 2010).....	25
<i>Quesada v. Banc of Am. Inv. Servs., Inc.</i> , 11-CV-01703 YGR, 2013 WL 623288 (N.D. Cal. Feb. 19, 2013).....	19
<i>Rodriguez v. Gates</i> , No. CV99-13190GAF(AJWX), 2002 WL 1162675 (C.D. Cal. May 30, 2002).....	15
<i>Romberio v. Unumprovident Corp.</i> , 385 F. App'x 423 (6th Cir. 2009) .....	15
<i>S. Bay Chevrolet v. GMAC</i> , 72 Cal. App. 4th 861 (1999) .....	22

**TABLE OF AUTHORITIES**  
(continued)

	<u>Page(s)</u>
<i>Sanders v. Apple Inc.</i> , 672 F. Supp. 2d 978 (N.D. Cal. 2009) .....	16
<i>Sarvis v. Gen. Dynamics Info Tech.</i> , 663 F. Supp. 2d 883 (C.D. Cal. 2009) .....	3
<i>Schulken v. Wash. Mut. Bank</i> , No. 09-CV-02708-LHK, 2012 WL 28099 (N.D. Cal. Jan. 5, 2012).....	26
<i>Sevidal v. Target Corp.</i> , 189 Cal. App. 4th 905 (2010) .....	24
<i>Stearns v. Ticketmaster Corp.</i> , 655 F.3d 1013 (9th Cir. 2011).....	24
<i>Wal-Mart Stores, Inc. v. Dukes</i> , 131 S. Ct. 2541 (2011) .....	1, 17, 19, 27
<i>Walter v. Hughes Commcn's, Inc.</i> , No. 09-2136 SC, 2011 WL 2650711 (N.D. Cal. July 6, 2011).....	19
<i>Wang v. Chinese Daily News, Inc.</i> , 709 F.3d 829 (9th Cir. 2013).....	15, 28
<i>Washington v. Joe's Crab Shack</i> , 271 F.R.D. 629 (N.D. Cal. 2010).....	28
<i>Webb v. Carter's Inc.</i> , 272 F.R.D. 489 (C.D. Cal. 2011) .....	24
<i>Whiteway v. FedEx Kinko's Office and Print Servs., Inc.</i> , No. C 05-2320, 2006 WL 2642528 (N.D. Cal. Sept. 14, 2006) .....	15
<i>Yeager v. Bowlin</i> , 693 F.3d 1076 (9th Cir. 2012).....	3
<i>Zinser v. Accufix Research Inst., Inc.</i> , 253 F.3d 1180 (9th Cir. 2001).....	28

**Rules**

Fed. R. Civ. P. 23 .....	17, 28
Fed. R. Civ. P. 23(a).....	1, 17, 27
Fed. R. Civ. P. 23(a)(2) .....	19
Fed. R. Civ. P. 23(a)(4) .....	24
Fed. R. Civ. P. 23(b)(2).....	passim
Fed. R. Civ. P. 23(b)(3).....	2, 27, 28

## I. INTRODUCTION

Plaintiffs have made no changes from their first motion that would satisfy the rigorous requirements of Rule 23 and place this case within the narrow “exception to the usual rule that litigation is conducted by and on behalf of the individual named parties only.” *Comcast Corp. v. Behrend*, 133 S. Ct. 1426, 1432 (2013) (quotation omitted). Once again, Plaintiffs cannot show that a single one of them relied on any statement by Apple when purchasing their devices, or that they—or any member of the proposed classes—ever experienced the hypothetical issues in their Complaint. And Plaintiffs continue to seek class certification under Rule 23(b)(2) to pursue “injunctive relief” that is entirely moot: (1) earlier this year, Apple stopped approving apps that call the UDID API, and iOS 7 (which was released yesterday and which any Plaintiff can freely download with a single click) eliminates the UDID API altogether; and (2) Plaintiffs’ geolocation allegations relate to a software bug that was fixed with a free Apple software update *over two years ago*. Recognizing that their claims are doomed, Plaintiffs raise a host of new theories that are deficient for the same reasons—and which may not serve as a basis for certification since they are nowhere pled in their Complaint.

**First**, the named Plaintiffs lack standing. Each admitted in sworn deposition testimony that he or she suffered ***no harm of any kind***. Moreover, during the February 28 hearing, this Court put Plaintiffs on notice that for their “overpayment” claims to survive, they need admissible evidence that a named Plaintiff *relied* on an alleged misrepresentation in purchasing a device—that is, saw the statement *before buying the phone and deemed it material to his or her purchasing decision*. Plaintiffs’ counsel admitted that Plaintiffs have “no evidence” of this, and that has not changed.

**Second**, Plaintiffs fail to satisfy the Rule 23(a) criteria. Plaintiffs’ proposed classes—their expanded “iDevice Class” and “Geolocation Class” and their newly minted “liability only” “Battery Life/Bandwidth Class”—are overbroad and unascertainable. Further, the named Plaintiffs are not typical or adequate since they were not injured and did not experience the challenged practices. Plaintiffs also fail to identify any *common evidence* capable of generating “common *answers* apt to drive the resolution of the litigation.” *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011). Quite the opposite: the evidence Plaintiffs cite—e.g., alleged “uneven enforcement” of non-consumer facing guidelines and “inconsistent application” of Apple’s “privacy policies to Apps”—



underscores the highly individualized and fact-specific circumstances that pervade Plaintiffs' claims. And Plaintiffs' own experts conceded that *they could not find a single example* of an app transmitting personal information from iOS (including in combination with a UDID) despite intensive analysis of more than 800 free apps, or of a user's "location data" being sent to Apple when Location Services was off, belying the possibility that there is "common evidence" of such practices.

**Finally**, Plaintiffs cannot satisfy the requirements to certify a class under Rule 23(b)(2) or (b)(3). They cannot obtain (b)(2) injunctive relief since they cannot establish a "continuing and imminent threat of harm"—or any harm. Apple already revised iOS to remove the ability for apps to access UDID and addressed the obscure software bug that is the subject of Plaintiffs' claims. And Plaintiffs have continued to buy and use Apple devices in the same way throughout the course of this litigation, defeating their claim that injunctive relief is needed. As for their newly proposed "liability only" (b)(3) class, Plaintiffs cannot meet (b)(3)'s demanding requirement that common issues "predominate" over individual ones or that their novel proposed class would be manageable or superior—since it presents countless individual inquiries into the resources used on a particular device and equally particularized causation inquiries. The Motion should be denied.<sup>1</sup>

## II. FACTUAL BACKGROUND—IDEVICE CLAIMS

The Complaint alleges that Plaintiffs used certain free apps that supposedly collected "personal information" from their devices and shared that data with third-party advertising or analytics companies, allegedly without their consent. Dkt. No. 104 ("TAC") ¶¶ 40–42, 44, 46, 82–87, 126–135. Plaintiffs allege that these apps used Application Programming Interfaces ("APIs") in iOS (Apple's mobile operating system) to obtain the unique device identifier ("UDID") associated with Plaintiffs' devices and transmitted these UDIDs together with "personal information" to specific third parties. TAC ¶¶ 82–83. Plaintiffs now have abandoned this theory and invented a host of new claims that appear nowhere in their Complaint. Critically, Plaintiffs still furnish no evidence that any of them was harmed by or personally experienced the challenged practices.

<sup>1</sup> Pursuant to the parties' stipulation of March 29, 2013, Apple produced 67,000 additional documents, identified by applying very broad search terms *proposed by Plaintiffs* to collections from 56 custodians *chosen by Plaintiffs, without reviewing the documents for responsiveness*. Yet Plaintiffs cite to new content in only 10 documents and *still* fail to make the necessary showings.

**A. Plaintiffs' Newly Expanded "iDevice Class"**

Previously, Plaintiffs proposed an "iDevice Class" consisting of iOS device owners running "iOS prior to 6.0" who had "downloaded one or more free Apps." Dkt. No. 189-1 at 13. Plaintiffs previously explained that they limited the proposed class in this manner because changes in iOS 6 addressed the concerns raised in their Complaint. Decl. of S. Ashlie Beringer ("Beringer Decl."), Ex. T, Feb. 28, 2013 Hearing Transcript ("Tr.") 12:2–22. Now, Plaintiffs propose a sweeping new class that includes anyone who acquired an iDevice after January 1, 2010—as many as 212 million individual users. Pls.' Br. ("Br.") at 8; Decl. of Mark Buckley ("Buckley Decl.") ¶ 33. Plaintiffs no longer require that class members downloaded any app, let alone one that collected personal information without permission. Nor do they limit the class to owners running pre-iOS 6.

**B. Named iDevice Plaintiffs**

There still is not a shred of evidence that even a single app transmitted "personal information" about the named Plaintiffs<sup>2</sup> to a third party or that Plaintiffs relied on any statement by Apple. Likewise, Plaintiffs make no attempt to show that they personally experienced any of the alleged practices, much less that they were harmed by them. Plaintiffs are unfit on every front:

- ***No Plaintiff relied on—or even reviewed—any statement made by Apple*** before purchasing his or her iPhone. *See* Beringer Decl., Ex. A (Chiu Dep. Tr. ("Chiu Dep.") 18:24–19:4; Ex. B (Dwyer Dep. Tr. ("Dwyer Dep.") 17:23–18:6; Ex. C (A. Capiro Dep. Tr. ("A. Capiro Dep.") 16:12–17:6; Ex. D (I. Capiro Dep. Tr. ("I. Capiro Dep.") 11:6–12.
- ***No Plaintiff considered privacy, security, resource allocation, or app access to data when making these purchases.*** Chiu Dep. 15:22–17:15; 18:18–19:4; 21:18–22:18; 25:5–16; Dwyer Dep. 14:3–15:7; 17:15–20; 25:5–14; 27:22–28:1; 31:24–32:21; A. Capiro Dep. 89:14–17; 128:3–18; I. Capiro Dep. 9:11–11:5.<sup>3</sup>
- ***Plaintiffs' experts concede that no Plaintiff actually had personal information collected from iOS by an app or had location information transmitted to Apple.*** Beringer Decl., Ex. F (Dr. Lodovico Marziale Dep. Tr. ("Marziale Dep.") 80:13–93:2 (conceding Complaint is unsupported); 93:24–94:25 (conceding no personal data was transmitted to a third party);

<sup>2</sup> Plaintiffs appear to argue for the first time that the Capiros should be representatives of the iDevice class. Br. 21–22. However, they did not plead this or offer evidence to support this.

<sup>3</sup> Although Plaintiffs' moving brief falsely asserts that a significant factor in their decision to purchase iPhones was a reliance on "Apple's promise to safeguard the privacy and security" of their personal data," Br. 11, their sworn deposition testimony flatly refutes this notion. *See infra* p. 3. Plaintiffs' sworn admissions control. *See, e.g., Sarvis v. Gen. Dynamics Info. Tech.*, 663 F. Supp. 2d 883, 894 (C.D. Cal. 2009); *Yeager v. Bowlin*, 693 F.3d 1076, 1080 (9th Cir. 2012).

112:25–117:4 (conceding data transmitted with Location Services off could not identify individuals or their location); Beringer Decl., Ex. E (Dr. Manuel Egele Dep. Tr. (“Egele Dep.”)) 165:20–25; 167:13–17 (admitting he conducted no analysis to determine if Plaintiffs experienced challenged practices); *see also* Decl. of Jeffrey Bolas (“Bolas Decl.”) ¶¶ 5, 63, 75, 100 (analysis of named Plaintiffs’ iPhones revealed no evidence of UDID transmission to third parties in Complaint or evidence that Location Services had ever been turned off).

- ***No Plaintiff can identify any harm*** that he or she experienced due to the practices alleged here—or even whether they personally experienced them. Chiu Dep. 104:13–24; 118:15–119:15; 140:10–142:25; Dwyer Dep. 243:12–16; 176:17–179:6; 180:14–183:11; A. Capiro Dep. 130:24–132:17; 135:11–19; 163:14–164:3; I. Capiro Dep. 91:3–21; 94:7–95:12.
- ***No Plaintiff can show that any UDID was or could have been used to contact or identify him or her or was combined with his or her personal information.*** In fact, during their testimony, Plaintiffs did not know what UDID was and could not identify any UDIDs associated with their devices. Dwyer Dep. 201:7–202:8; Chiu Dep. 106:24–110:20; 112:18–113:2; A. Capiro Dep. 131:7–14; I. Capiro Dep. 92:9–94:5. And Plaintiffs’ expert, Dr. Egele, could not find a single example of a UDID being combined with personal information despite months of analysis of more than 800 free apps in the App Store. Egele Dep. 230:9–18; 216:13–17.
- ***All Plaintiffs benefited from using free apps and Location Services***, including from the ability of certain apps to collect data from their iPhones. Dwyer Dep. 139:5–141:12; Chiu Dep. 100:6–21; I. Capiro Dep. 46:24–47:14; 77:3–89:19. And all continued to use apps and Location Services without regard for the potential data collection impact throughout the litigation. Chiu Dep. 116:11–20; Dwyer Dep. 35:19–39:10; I. Capiro Dep. 48:21–49:5.
- ***All Plaintiffs continued to purchase iPhones after filing their claims.*** Dwyer Decl. ¶ 5; Chiu Decl. ¶ 5; A. Capiro Decl. ¶ 3; I. Capiro Decl. ¶ 4; Buckley Decl. ¶¶ 25–30.
- ***All Plaintiffs have devices with the capability to upgrade to iOS 7*** (released yesterday), and therefore can remove apps’ ability to access UDID entirely. Buckley Decl. ¶¶ 25–30; Decl. of Erik Neuenschwander (“Neuenschwander Decl.”) ¶ 7, 29.

Tellingly, Plaintiffs have abandoned their central claim that specific apps collected and transmitted their personal data to third parties without consent, undoubtedly because there is no evidence to support their allegations. Indeed, although Plaintiffs Chiu and Dwyer alleged that five apps transmitted 60 pieces of information to third-party advertisers, their own experts conceded there is no evidence of this—or that any app ever sent their personal data. *See* TAC ¶¶ 41–42; Bolas Decl. ¶¶ 5, 63, 75; Appendix A (summary of allegations and forensic analysis); Marziale Dep. 71:2–74:11; 77:12–23; 78:21–80:11; 80:13–93:2; 93:24–94:25; Egele Dep. 230:9–18; 216:13–17.

### C. Alleged Misrepresentations and Omissions

Plaintiffs have abandoned their core misrepresentation claim (*see* Tr. 6:14–17) and pivoted to

two new “misrepresentations” that are not pled in their TAC and that no Plaintiff ever relied on.<sup>4</sup> Plaintiffs again offer no evidence—much less common evidence—to support these new claims.

### 1. UDID as “Non-Personal Information”

Plaintiffs for the first time argue that Apple’s Privacy Policy (incorporated into Apple’s Software License Agreement (“SLA”)) “falsely” defines UDID to be “non-personal information.” Br. 4, 8. This argument is illogical. Most basically, the Privacy Policy extends only to *Apple’s* own collection and use of data—i.e., “how *we* collect, use, disclose, transfer, and store your information”—and expressly excludes the practices of third parties, such as apps. Decl. of Jane Horvath (“Horvath Decl.”) ¶ 8. Apple defines “personal information” as “data that can be used *to uniquely identify or contact a single person*,” such as “name, mailing address, [and] phone number.” *Id.* In contrast, Apple identifies “non-personal information” as “data in a form that does not permit direct association with any specific individual,” including “zip code, area code [and] *unique device identifier*.” *Id.* (emphasis added). It also explains that “[i]f [Apple] combine[s] non-personal information with personal information, the combined information will be treated as personal information *for as long as it remains combined*.” *Id.* (emphases added).

Plaintiffs offer no evidence that Apple’s definition of UDID—an alphanumeric hexadecimal string that (like a serial number) identifies a device—in its Privacy Policy is in any way “false.” Indeed, Plaintiffs do not cite a single example of a UDID that (i) was or could ever have been used to uniquely identify or contact one of them, or (ii) was ever combined with any of their personal information. *Supra* p. 4. ***Plaintiffs’ experts also agree that UDID alone is not personal information*** that can uniquely identify any individual. *See* Egele Dep. 31:5–10; Marziale Dep. 32:1–33:1; 78:21–79:5 (“I certainly can’t go from this data to an individual person.”). And after months of analysis of hundreds of free apps, ***Plaintiffs’ expert did not find a single example of an app combining UDID with personal information***. *See* Egele Dep. 230:9–18.

The three internal Apple emails cited by Plaintiff (Br. 8–9) provide no support for this theory.

<sup>4</sup> Plaintiffs reference a litany of other purported statements from Apple (*see* Br. 3), but there is *no* specific discussion of most of these statements in the remainder of Plaintiffs’ motion (much less an explanation of how they are false, how Apple has purportedly breached them, whether and how Plaintiffs relied on (or if they were even aware of) these statements, etc.). These bare references cannot provide any viable foundation for class certification and must be disregarded.

The first simply confirms that in specific cases, UDID could be personal information *if aggregated* with personally identifiable data. *See* Kravitz Decl. Ex. 28. The second *highlights* that Apple handles apps discovered to be transmitting UDID in the same way that it treats apps collecting personal information—not because UDID *is* personal data, but to mitigate the risks of UDID being combined with personal information. *See id.* Ex. 29. And the final email discusses a different and irrelevant identifier. *See id.* Ex. 30; Neuenschwander Decl. ¶ 14. Plaintiffs simply ignore mountains of evidence confirming that Apple viewed the bare UDID, not coupled with personal information, as *device*—not personal or user—information. *See, e.g.,* Beringer Decl., Exs. L, P; Ex. H (Shoemaker Dep. Tr. (“Shoemaker Dep.”)) 50:8–14; Ex. I (Geleynse Dep. Tr. (“Geleynse Dep.”)) 42:15–22.

## 2. Promise to Use SSL Encryption on Apple Web Pages

Plaintiffs now also point to a provision in Apple’s Privacy Policy that “*Apple online services* such as the Apple Online Store and iTunes Store use Secure Sockets Layer (SSL) encryption *on all web pages where personal information is collected.*” Br. 12 (emphasis supplied). Plaintiffs contend that this is “false” based on a single putative example of an allegedly unencrypted transmission triggered by *the Pandora App*—not the user interacting with an Apple web page—to the iTunes server from Plaintiff Chiu’s phone. Br. 12–13. This unpled theory is baseless. Most fundamentally, there is no evidence that this transmission was not encrypted, and Dr. Marziale gives no foundation for his purported encryption analysis. In fact, such transmissions are routinely encrypted. Neuenschwander Decl. ¶ 32. Separately, the transmission of a UDID to iTunes triggered by an app does not implicate Apple’s Privacy Policy, since this does not involve Apple’s collection of personal data via a user’s direct interaction with an Apple “web page.” Horvath Decl. ¶¶ 12–14.

## D. Plaintiffs’ New Critiques of Apple’s Business and Technology

Plaintiffs also raise two new arguments unrelated to any consumer representation. They again tie neither of these vague complaints to any named Plaintiff or any common practice or evidence.

### 1. “Uneven Enforcement” of the PLA and App Review Guidelines

First, Plaintiffs argue that Apple “selectively enforce[s]” the iOS Developer Program License Agreement (“PLA”) and App Store Review Guidelines (non-public contracts applicable solely to app developers) by failing to “regularly test apps to determine if they are improperly calling UDIDs or

1 making proper disclosures” or “look for” many unspecified “things that are required to protect user  
 2 privacy.”<sup>5</sup> Br. 11, 12; Decl. of Phillip Shoemaker (“Shoemaker Decl.”) ¶¶ 7-10. Plaintiffs offer no  
 3 *evidence* of “selective enforc[ement],” however, and they do not identify a ***single instance*** where  
 4 Apple failed to enforce a known violation of its App Review Guidelines. Instead, Plaintiffs cite a few  
 5 emails that illustrate the contextual and fact-intensive nature of Apple’s app review process and the  
 6 challenges of manually reviewing millions of apps submitted to Apple each year.

7 [REDACTED]  
 8 [REDACTED]  
 9 [REDACTED]  
 10 [REDACTED]  
 11 [REDACTED]  
 12 [REDACTED]  
 13 [REDACTED]  
 14 [REDACTED]  
 15 [REDACTED]  
 16 [REDACTED]  
 17 [REDACTED]  
 18 [REDACTED]  
 19 [REDACTED]  
 20 [REDACTED]  
 21 [REDACTED]  
 22 [REDACTED]  
 23 [REDACTED]  
 24 [REDACTED]  
 25 [REDACTED]

26 <sup>5</sup> Plaintiffs appear to suggest that Apple’s enforcement scheme related to third-party apps’ data  
 27 practices somehow implicates Apple’s Privacy Policy. Br. 3–4. This is wrong. The Privacy  
 28 Policy by its terms describes ***Apple’s*** handling of ***user data***; it expressly states that it does not  
 cover the data collection practices of third-party apps that may run on iOS devices. Horvath  
 Decl. ¶¶ 8–11.

## 2. Complaints About Device Resource Depletion

Plaintiffs also invent a new theory of liability—untethered to any alleged misrepresentation—related to “the diminishment of resources, premature degradization [sic] of the battery and free use of the class member’s bandwidth.” Br. 14–15. Plaintiffs suggest that resource usage is an *independent wrong* giving rise to a separate cause of action, whether or not tied to unauthorized data transmission. *Id.* Not surprisingly, Plaintiffs offer no proof that they (or anyone) experienced resource depletion, much less due to unauthorized data transmissions by third-party apps. Instead, Plaintiffs cite only inapposite testimony by Dr. Egele and two emails that discuss authorized battery use resulting from *users’* explicit behavior. *See id.*; Kravitz Decl. Ex. 20 (battery drain after *authorizing* Location

<sup>6</sup> Plaintiffs mischaracterize two emails by Mr. Shoemaker, asserting that they somehow show evidence of “breaches of Apple’s representations to end users.” Br. 12, Kravitz Decl. Exs. 25 & 6. But Plaintiffs cite no representation made to consumers about app review—and there is none. Moreover, these emails speak to the resource constraints that would make it impossible for Apple to “actively look[]” for UDID violations—which would require a “four-hour [technical investigation] process to be done on every single app.” Shoemaker Dep. 178:13–18; Shoemaker Decl. ¶¶ 23, 73.



Services); Ex. 21 (battery drain *upon downloading an app*). Similarly, Plaintiffs’ reliance on a draft article about “energy bugs” is misplaced, since these “bugs” result from causes entirely unrelated to third-party apps collecting or transmitting user data. Br. 14, Kravitz Decl. Ex. 22. Likewise, in support of their bandwidth claim, Plaintiffs cite inapposite emails about *traffic* data, not cell tower and Wi-Fi data. Br. 14–15, Kravitz Decl. Ex. 24; Decl. of Ronald Huang (“Huang Decl.”) ¶ 36.

Plaintiffs do not even attempt to show that they personally suffered an adverse impact to their bandwidth, storage capacity, or battery life due to the alleged data transmissions. *See supra* pp. 3–4. And despite Dr. Egele’s contradictory declaration, he conceded that he made *no attempt* to determine whether Plaintiffs—or anyone—experienced diminished resources due to the challenged data transmissions. Egele Dep. 165:20–166:4; 167:4–25; 185:14–186:20; 187: 8–13; 193:19–195:1.

**E. The Proposed Injunctive Relief Was Mooted by iOS Changes Beginning with iOS 5**

Plaintiffs seek to represent an “injunctive relief” class under Rule 23(b)(2) in an effort to impose a series of misguided changes to Apple’s app review practices, developer policies, and operating system. Br. 10–15. Among other flaws, the proposed “relief” is entirely mooted by changes Apple voluntarily implemented beginning with iOS 5, which was released in the fall of 2011. Consistent with its ongoing efforts to improve its products, Apple deprecated UDID in iOS 5 and began to transition developers away from the UDID API, removing developer access to UDID altogether in iOS 7. Neuenschwander Decl. ¶¶ 18, 21–22, 27, 29. Indeed, Plaintiffs’ expert conceded that Apple is the *only mobile platform* to implement non-persistent identifiers supporting legitimate app functions and avoiding privacy risk. Egele Dep. 131:5–135:4; Neuenschwander Decl. ¶¶ 19, 21. In iOS 6, Apple implemented new, non-persistent identifiers that avoid any concerns with UDID along with controls that prevented apps from accessing personal information (such as photos or contacts) from iOS without first obtaining the user’s express consent. Neuenschwander Decl. ¶ 25.

Apple’s transition to these new identifiers—and removal of the UDID API—is now complete. On May 1, Apple began rejecting all apps attempting to access UDID, even with user consent. Shoemaker Decl. ¶¶ 39–40. And iOS 7, released yesterday, removes the ability of apps to access UDID (and a more basic, low-level identifier, MAC Address) altogether. Beringer Decl., Ex K (E. Neuenschwander Dep. Tr.) 109:12–20; Neuenschwander Decl. ¶¶ 26, 29. Notably, each Plaintiff—



1 and the majority of all iOS device owners—can upgrade to iOS 7 in seconds at no cost. *Id.* ¶ 28.

### 2 III. FACTUAL BACKGROUND—GEOLOCATION CLAIMS

#### 3 A. Plaintiffs’ Previously Proposed “Location Services ‘Off’ Class” and Their Newly 4 Expanded “Geolocation Class”

##### 5 1. The Newly Defined Proposed Geolocation Class

6 Plaintiffs previously sought to certify a “Location Services ‘Off’ Class” consisting of anyone  
7 in the United States who turned Location Services off on their device between “June 21, 2010  
8 through April 27, 2011” and then “had location information when location services were ‘off’  
9 transmitted to Apple’s servers.” Dkt. No. 138. Plaintiffs now seek to redefine their proposed class to  
10 consist of all users who “turned location services ‘off’ and had their device collect, store, and/or  
11 transmit geolocation data” at any time since January 1, 2008—an expansion of the class period from  
12 a period of months to almost six years. Br. 8. Ascertaining this proposed class would require an  
13 impossible inquiry into whether hundreds of millions of users who may have turned Location  
14 Services off “had their device collect, store and/or transmit geolocation data.” *Id.* Critically, Apple  
15 has no records of when or whether a user turns Location Services off, or of what data may have been  
16 collected, stored, or transmitted from the user’s device if it was. Huang Decl. ¶ 19.

##### 17 2. Plaintiffs’ Geolocation Allegations

18 The Geolocation Plaintiffs assert UCL and CLRA claims alleging that unspecified “location  
19 information” was transmitted from Isabella Capiro’s iPhone to Apple’s servers after she turned  
20 Location Services off, supposedly in violation of Apple’s SLA. TAC ¶¶ 29-30, 163. Specifically,  
21 Plaintiffs claim that Apple breached the provision advising, “You may withdraw this consent [to  
22 Apple’s . . . transmission, collection, maintenance, processing and use of *your location data*] at any  
23 time by . . . either turning off the global Location Services setting or turning off the individual  
24 location settings of each location-aware item on your iOS Device.” *See* Br. 16; Buckley Decl. ¶ 8,  
25 Exs. A–D (emphasis added).

26 Plaintiffs’ claims are directed to certain versions of iOS 4 containing a harmless, obscure bug  
27 that potentially (in highly fact-specific circumstances) caused an iPhone to begin requesting data  
28 needed to determine its own location even if Location Services was off. Huang Decl. ¶¶ 11-13.  
However, as explained below (*infra* p. 11), Plaintiffs’ own expert concedes that no location data

(much less a user's location data) was ever transmitted to Apple as part of this process. Huang Decl. ¶ 16; Egele Dep. 158:15–159:17; 165:2–19; *see also* Marziale Dep. 116:7–117:3; 109:9–110:18. Plaintiffs do not (and cannot) offer any evidence that Plaintiffs' or any user's location information was sent to Apple (or collected or stored on the device) when Location Services was off, and they concede that this bug was resolved in a free iOS update Apple released in May 2011 and in later iOS versions, including those that each Plaintiff downloaded. Br. 18; Huang Decl. ¶¶ 24, 27.

#### **B. Named Geolocation Plaintiffs**

Critically, none of the Plaintiffs had their location data transmitted to Apple with Location Services off.<sup>7</sup> A. Capiro Dep. 20:17–22; 163:14–164:3. Likewise, neither of the Capiros—who first used iPhones running iOS 4.2.1—ever used a pre-iOS 4 version capable of engaging in “geo-tagging” (which Plaintiffs raise in their motion but not in their Complaint) while Location Services was off. Buckley Decl. ¶¶ 25–28; Huang Decl. ¶¶ 22–24. More fundamentally, neither Capiro Plaintiff knew about Location Services or the SLA—or considered location features or privacy—when Mr. Capiro purchased their iPhones. A. Capiro Dep. 16:12–17:6; I. Capiro Dep. 11:6–12, 72:18–20.

Although Isabella Capiro testified that she turned Location Services off on a handful of occasions, she cannot remember even generally when she may have done so, including whether she did so before upgrading to iOS 4.3.3 (which resolved the bug). I. Capiro Dep. 43:15–24; 44:16–45:21; Buckley Decl. ¶ 27. And a forensic analysis of Ms. Capiro's devices revealed that she had Location Services “On” and authorized numerous apps to access location throughout the relevant time period—consistent with her admitted practice. Bolas Decl. ¶¶ 93–96; I. Capiro Dep. 60:16–61:8; 74:24–88:6; 57:23–58:2; A. Capiro Dep. 20:17–22.

Unsurprisingly, the Capiros have no evidence that any data (much less “location data”) was ever sent from their iPhones when Location Services was off to Apple or to anyone else, and they concede they were in no way harmed even if it was. I. Capiro Dep. 101:9–14; 91:11–21;

<sup>7</sup> The Complaint alleges that only the Capiro Plaintiffs are proposed Geolocation Class representatives—and never alleges that the separate iDevice Plaintiffs are encompassed by the Geolocation claims. Indeed, Plaintiff Dwyer testified that he was considered but rejected as a class representative for the Geolocation Class, perhaps because he only turned Location Services off on airplanes, when it would not be possible to transmit data. Dwyer Dep. 141:2–7; 172:18–173:20. And Plaintiff Chiu testified that he routinely turns Location Services on to enjoy his iPhone's location-based features. Chiu Dep. 79:21–81:13; 88:15–89:13; 101:7–14.

94:7–95:12; 97:12–17; 91:3–9; A. Capiro Dep. 131:23–132:17; 135:11–19. In fact, the Capiros have long since upgraded to iOS 4.3.3 or later versions. Buckley Decl. ¶¶ 27–28.

### C. iOS 4 Bug Triggered Rarely and in Highly Fact-Specific Circumstances

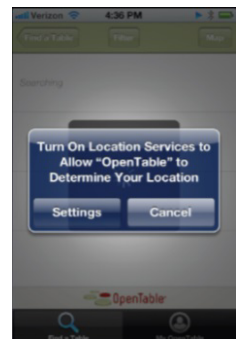
#### 1. No Transmission of “Your Location” Data

Plaintiffs’ geolocation claims relate to a software bug that existed in certain versions of iOS 4 prior to the release of iOS 4.3.3 on May 3, 2011. Huang Decl. ¶ 11. Users may consent to provide their current location to apps (or to Apple) to receive a variety of location-based services. *Id.* ¶¶ 2–4. The device itself determines its own location, utilizing local “maps” it requests from Apple that allow it to estimate its whereabouts. *Id.* ¶¶ 11–12. In limited and specific circumstances, an iOS device (before 4.3.3) could begin the process of calculating its approximate location when a user opened an app that made a specific type of location request, even if Location Services was off. Specifically, the device might send a list of identifiers for publicly broadcasting Wi-Fi routers in its range to Apple’s servers. *Id.* ¶ 5. Without storing this request, Apple’s servers immediately looked up and returned the equivalent of a “map” to the device—i.e., the rough locations of those towers and routers, along with other routers and towers as far as 100 miles away. *Id.* ¶¶ 6–10. Using that “map,” the device could then estimate its own location—*although it never sent that device’s location to Apple, or any app or third party, if Location Services was off.* *Id.* ¶¶ 11–12.

Importantly, this bug was not actually triggered for all or even most iPhone users running iOS 4.1–4.3.2 who turned Location Services off. *Id.* ¶¶ 11, 15–16. To know whether data actually was transmitted to Apple servers from a particular device, it would be necessary to answer a number of questions concerning the specific device, device location, and user and app behavior. *Id.* ¶ 15.

#### 2. No Impact on Location Services Setting

Plaintiffs now assert (without any factual support) that Apple failed to honor the Location Services setting. Br. 2. This setting is handled entirely on the device and controls whether the user’s real-time location may be sent to apps or services that request it. Huang Decl. ¶ 2. As shown here, if Location Services is off and an app requests the user’s location, iOS displays a prompt that notifies users that they must “Turn On Location Services To Allow [The App] To



Determine Your Location.” Plaintiffs do not and cannot point to a single instance when an app or service was able to “determine [a user’s] location” when the Location Services setting was off—and there is none. *Id.* ¶¶ 12, 16. Even when the iOS 4.1–4.3.2 bug was in effect, the Location Services setting functioned as intended, and iOS never provided a user’s location to an app. *Id.*

**D. Plaintiffs’ Newly Invented Geo-tagging Theory (Based on Pre-iOS 4.1)**

Having learned that their Geolocation Claims are baseless, Plaintiffs pivot to a new theory relating to “geo-tagging” for users of “iOS version 4.0 or earlier”—versions Plaintiffs never used. Br. 17. This theory rests on wildly speculative, false, and unsupported assertions. For example, Plaintiffs contend that for users of “iOS version 4.0 or earlier,” Apple “shared and continues to share [data with] Google and/or Skyhook, regardless of whether Location Services is . . . ‘off.’” *Id.* Plaintiffs cite no evidence for this false claim. Huang Decl. ¶¶ 20–21. They also make unfounded claims that Apple “collect[ed] detailed location data from all iDevice users” for “geo-tagging.” Br. 16–17. But Plaintiffs do not offer any evidence of this and do not even identify what “detailed location data” Apple purportedly collected in “geo-tagging”—and there is none. Huang Decl. ¶ 23.

**IV. NO CLASS CAN BE CERTIFIED BECAUSE PLAINTIFFS LACK STANDING**

“[N]o class may be certified that contains members lacking Article III standing.” *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 594 (9th Cir. 2012) (quotations omitted); *see also Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F.3d 1018, 1022–23 (9th Cir. 2003). Moreover, for injunctive standing under Article III, the “analysis must . . . focus exclusively on whether there exists a threat of future harm as to” the named Plaintiffs. *Nelsen v. King Cnty.*, 895 F.2d 1248, 1251 (9th Cir. 1990). And allegations are not enough: “On a motion for class certification, Plaintiffs must demonstrate, *not merely allege*, that they have suffered an injury-in-fact to establish Article III standing to bring the claims asserted on behalf of” the putative class. *Evans v. Linden Research, Inc.*, No. C 11-01078 DMR, 2012 WL 5877579, at \*6 (N.D. Cal. Nov. 20, 2012) (emphasis added) (citation omitted).

The named Plaintiffs have conceded in sworn deposition testimony that (i) they were not harmed by Apple’s alleged conduct in any way; (ii) they did not experience any impairment to device resources; (iii) they did not review or rely on any statement by Apple when purchasing their iPhones; and (iv) they have no evidence that they, themselves, experienced the challenged practices. *Supra* pp.

3–4. Each lacks standing, and class certification must be denied on this basis alone. *See, e.g., Birdsong v. Apple, Inc.*, 590 F.3d 955, 960–61 (9th Cir. 2009).

In fact, at the February 28, 2013 hearing, this Court pointedly asked how Plaintiffs could demonstrate standing based on an overpayment/reliance theory when all of them *admitted* that they had never seen any alleged misrepresentation *before* purchasing their iDevices. *See* Tr. at 37:7–10 (“The Court: Give me any evidence that anyone [read the statements] before they bought the phone, that class members would have looked at an iTunes Terms and Conditions Privacy Policy before they bought the iDevice.”). Plaintiffs’ counsel admitted: “I have no evidence.” *Id.* at 37:11–12.

Plaintiffs now submit amended declarations attempting to walk away from their previous deposition testimony and arguing that their admissions that they suffered no harm did not relate to their “overpayment” theory. *See, e.g.,* Amended Dwyer Decl. (Dkt. No. 245-2), ¶ 12; Amended Chiu Decl. (Dkt. No. 244-14), ¶ 15 (same). But these amended declarations only *confirm* Plaintiffs’ lack of standing: ***Despite their attempted backtracking, none of the Plaintiffs contend that they saw, relied on, or considered material to their purchasing decision an alleged Apple misrepresentation before they bought their iPhones.***<sup>8</sup> This is the evidentiary end of Plaintiffs’ manufactured “overpayment” theory of standing. *See, e.g., In re Google Android Consumer Privacy Litig.*, No. 11-MD-02264 JSW, 2013 WL 1283236, at \*6 (N.D. Cal. Mar. 26, 2013) (no standing if plaintiffs “[did] not identify what statements were material to their [purchase] decision”); *In re LinkedIn User Privacy Litig.*, No. 12-CV-03088 EJD, 2013 WL 844291, at \*4 (N.D. Cal. Mar. 6, 2013).

Plaintiffs also lack standing to pursue *injunctive* relief because they cannot “establish the basic requisites of . . . the likelihood of substantial and immediate irreparable injury, and the inadequacy of remedies at law.” *O’Shea v. Littleton*, 414 U.S. 488, 502 (1974); *Jenkins v. Apple Inc.*, No. 11-CV-01828-LHK, 2011 U.S. Dist. LEXIS 71261, at \*5-6 (N.D. Cal. July 1, 2011) (no Art. III injunctive standing where “*Plaintiffs acknowledge that their claims are based entirely on past transactions, and concede that they do not face any realistic threat of future injury from Apple’s allegedly unfair business practices*”); *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013)

<sup>8</sup> The redline comparisons of Plaintiffs’ initial declarations and their amended declarations are attached as an exhibit to the Beringer Declaration. *See* Beringer Decl., Ex. G.

1 (“[a]llegations of *possible* future injury’ are not sufficient”); *City of Los Angeles v. Lyons*, 461 U.S.  
 2 95, 96 (1983) (no standing to seek injunctive relief where “speculative nature of his claim that he will  
 3 again experience injury as the result of that practice even if continued”).

4 Here, Plaintiffs have failed to establish any realistic threat of future injury. Among other  
 5 things, (1) Apple stopped approving any apps that call UDIDs, and iOS 7 (which any Plaintiff can  
 6 now freely download with a single click) eliminates the UDID API altogether; and (2) Plaintiffs’  
 7 geolocation allegations relate to a bug that was fixed with a free software update from Apple *over two*  
 8 *years ago*. Neuenschwander Decl. ¶¶ 24, 26–29; Huang Decl. ¶¶ 13, 17, 27. Finally, since each  
 9 Plaintiff (other than Mr. Dwyer, who states that he no longer uses an iPhone and for that independent  
 10 reason lacks standing to pursue injunctive relief<sup>9</sup>) continues to use free apps and Location Services,  
 11 they plainly do not believe they face any threat of future injury. *See* Beringer Decl., Ex. S.

#### 12 **V. THE PROPOSED CLASSES ARE OVERBROAD AND NOT ASCERTAINABLE**

13 Class certification also must be denied because the proposed classes are vastly overbroad and  
 14 not “precise, objective, and presently ascertainable.” *Mazur v. eBay, Inc.*, 257 F.R.D. 563, 567 (N.D.  
 15 Cal. 2009). The class definition must be “sufficiently definite” so that “members can be ascertained  
 16 by reference to objective criteria.” *Whiteway v. FedEx Kinko’s Office and Print Servs., Inc.*, No. C  
 17 05-2320, 2006 WL 2642528, at \*3 (N.D. Cal. Sept. 14, 2006). Courts repeatedly have denied class  
 18 certification where ascertaining membership would require “individualized fact-finding” or make a  
 19 “determination of the merits of the individual claims to determine whether a particular person is a  
 20 member of the class.” *Romberio v. Unumprovident Corp.*, 385 F. App’x 423, 431 (6th Cir. 2009);  
 21 *Carrera v. Bayer Corp.*, No.12-2621, 2013 U.S. App. LEXIS 17479, at \*6 (3d Cir. Aug. 21, 2013).

22 The ascertainability requirement applies not only to a proposed (b)(3) class, but also to a  
 23 proposed (b)(2) class, where it is essential to assessing whether the proposed injunction applies to  
 24 conduct experienced uniformly by all members of the class and would benefit each class member  
 25 equally. *See, e.g., Rodriguez v. Gates*, No. CV99-13190GAF(AJWX), 2002 WL 1162675, at \*9  
 26 (C.D. Cal. May 30, 2002) (denying 23(b)(2) certification for lack of ascertainable class definition).

27  
 28 <sup>9</sup> *See* Kravitz Decl. Ex. 2 ¶ 5; *see also Wang v. Chinese Daily News, Inc.*, 709 F.3d 829, 835 (9th  
 Cir. 2013).



Each of Plaintiffs' classes fails to meet the ascertainability requirement.

First, Plaintiffs' newly defined "iDevice Class" gives new meaning to the term "overbroad," as it encompasses everyone in the U.S. who acquired an iDevice after January 1, 2010. Br. 8. This is *hundreds of millions of people*, including millions (like the Plaintiffs) who never had "personal information" collected by a third-party app or "tracking" company, never reviewed or relied upon any alleged misrepresentation, never used an app, and never suffered harm. *See Mazza*, 666 F.3d at 594; *Sanders v. Apple Inc.*, 672 F. Supp. 2d 978, 991 (N.D. Cal. 2009) (proposed class "necessarily includ[ing] individuals . . . who either did not see or were not deceived by advertisements, and individuals who suffered no damages" unascertainable). Plaintiffs have even dropped their previous condition that class members must have downloaded a free app. *See* Tr. at 36:9–11 (Mr. Kamber: "[T]he only way you are [an iDevice class member] is if you . . . downloaded a free app.").

Second, the putative "Geolocation Class" fails because it would be impossible to determine who turned Location Services off during the relevant time period or whether any data was transmitted to Apple (or collected or stored on the device) when this setting was off. *See, e.g., Mazur*, 257 F.R.D. at 567-68 (proposed class "wholly unascertainable" where plaintiffs could not identify a "method by which to determine how to identify" class members); *Hanni v. Am. Airlines, Inc.*, No. C 08–00732 CW, 2010 WL 289297, at \*9 (N.D. Cal. Jan. 15, 2010).

Finally, Plaintiffs' "liability-only" "Battery Life/Bandwidth Class" is the biggest stretch of them all. To determine membership, it would be necessary to assess, among other things, whether an individual (i) "experienced shortened battery life" *or* (ii) experienced "increased bandwidth usage" (iii) *as a result of* (iv) Apple's "unauthorized" use of Location Services, *or* (v) "Apple's misrepresentations and omissions regarding unauthorized transmissions" (meaning the existence of an actual misrepresentation, reliance, and specific app activity, among myriad other individualized factors). Br. 24–27. To even list these (non-exhaustive) criteria is to make plain that membership in this proposed class could never be determined—and certainly not without "extensive and individualized fact-finding or 'mini-trials.'" *Carrera*, 2013 U.S. App. LEXIS 17479, at \*6.

## **VI. PLAINTIFFS CANNOT CERTIFY A CLASS BASED ON UNALLEGED THEORIES**

It is axiomatic that Plaintiffs cannot certify a class based on theories and claims not pled in the

operative complaint (*see, e.g., Evans v. IAC/Interactive Corp.*, 244 F.R.D. 568, 571 (C.D. Cal. 2007))—a point this Court made at the February hearing. *See* Tr. at 59:3–4, 10–12. Yet, Plaintiffs attempt to do this.<sup>10</sup> *See* Beringer Decl., Ex. U (chart listing all theories appearing for the first time in Second Class Certification brief). Plaintiffs cannot amend their pleadings through their class certification briefing; they are restricted to claims they have alleged. *See Evans*, 244 F.R.D. at 571.

## VII. PLAINTIFFS CANNOT SATISFY THE REQUIREMENTS OF RULE 23(A)

The Supreme Court’s controlling decision in *Dukes* established that “Rule 23 does not set forth a mere pleading standard”; rather, “[a] party seeking class certification must affirmatively demonstrate his compliance with the Rule—that is, he must be prepared to prove that there are *in fact* sufficiently numerous parties, common questions of law or fact, etc.” *Id.* at 2551. Specifically, Plaintiffs must present evidence demonstrating the four prerequisites of Rule 23(a)—“typicality,” “commonality,” “adequacy of representation,” and “numerosity”—in addition to Rule 23(b)(2)’s requirements. *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 979-80 (9th Cir. 2011). In turn, the Court must conduct a “rigorous analysis” of Plaintiffs’ evidence that will “[f]requently . . . entail some overlap with the merits of the plaintiff’s underlying claim.” *Dukes*, 131 S. Ct. at 2551.

### A. The Named Plaintiffs—Who Suffered No Injury, Had No Data Transmitted, Are Not Concerned by and Continue to Engage in the Challenged Practices—Are Not Typical

Plaintiffs cannot demonstrate typicality, which focuses on “whether other [class] members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured by the same course of conduct.” *Ellis*, 657 F.3d at 984 (citation omitted). *First*, each Plaintiff lacks standing under Article III, the UCL, and CLRA (*supra* pp. 133-15), defeating typicality. *See, e.g., Cholakyan v. Mercedes-Benz USA, LLC*, 281 F.R.D. 534, 557 (C.D. Cal. Mar. 28, 2012). *Second*, none of the Plaintiffs experienced the “same course of conduct” or “the same or similar injury,” *Ellis* at 984, as the proposed classes:

- Plaintiffs concede ***they did not review or rely on any representation*** in Apple’s Privacy Policy or SLA—or consider privacy—when purchasing their iPhones. *Supra* p. 3; *Aberdeen v. Toyota*

<sup>10</sup> If the Court permits Plaintiffs to pursue these theories, Apple requests an opportunity to depose Plaintiffs and their experts on each of the new theories raised in their motion.



*Motor Sales, U.S.A.*, No. CV-08-1690-PSG, 2009 WL 7715964, at \*6 (C.D. Cal. June 23, 2009) (denying UCL and CLRA certification; “[b]ecause Plaintiff did not view [the] allegedly deceptive advertisements prior to purchasing . . . his claims are clearly not typical of consumers who saw and relied on those ads”), *aff’d in relevant part*, 422 F. App’x 617, 618 (9th Cir. 2011); *Endres v. Wells Fargo Bank*, No. C 06-7019 PJH, 2008 WL 344204, at\*6 (N.D. Cal. Feb. 6, 2008).

- There is ***no evidence that any free app ever collected or transmitted “personal information” from Plaintiffs’ devices*** to a third-party “tracking” company. *Supra* pp. 3–4. And the parties and their experts are ***in agreement that UDID is not “personal information.”*** *Id.* There is no evidence that any UDID associated with their devices (i) was or could have been used to uniquely identify or contact them or (ii) was ever combined with any personal information. *Supra* p. 4. Plaintiffs’ counsel conceded as much. *See* Tr. at 79:6–7 (Mr. Kamber: “Otherwise [an identifier is] just a number until it’s a number with other things.”).
- ***No Plaintiff even alleges, let alone shows, that Apple collected personal information through a web page on which Apple failed to use SSL encryption.*** Plaintiff Chiu’s allegation that Pandora sent unencrypted personal information to iTunes is (i) unrelated to Apple’s representations about collection of information through its webpages, (ii) concerns UDID, which is non-personal information, and (iii) lacks evidentiary support. Neuenschwander Decl. ¶ 32.
- ***Plaintiffs admit that they did not experience unauthorized resource consumption or any other harm as a result of any alleged practices.*** A. Capiro Decl. ¶ 54, 131:15–144; I. Capiro Decl. ¶ 17, 30:1; 34:8; 91; 100; Chiu Decl. ¶ 20, 146-151; Dwyer Decl. ¶ 33; 73; 243; 250.
- ***No Plaintiff is running “legacy apps” on a device*** that cannot update to the new iOS version in which UDID is no longer accessible to apps. Dwyer Decl. ¶ 5 (iPhone 5); Chiu Decl. ¶ 5 (iPhone 4S); A. Capiro Decl. ¶ 7 (iPhone 4); I. Capiro Decl. ¶ 3 (iPhone 4S); Buckley Decl. ¶¶ 25–30.
- ***No Plaintiff has been affected by unauthorized “geo-tagging”*** since no named Plaintiff has both used a pre-4.1 version of iOS and turned Location Services off. Buckley Decl. ¶¶ 25-28 (Capiros running 4.2.1); Marziale Decl., ¶ 13 (Dwyer running 5.1.1., Chiu running 5.2); Huang Decl. ¶ 24 (geo-tagging bug affects only iOS versions prior to 4.1).

Nor do Plaintiffs’ interests align with those of the proposed classes, the essential “purpose of the typicality requirement.” *Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992).

Plaintiffs do not share or even understand the privacy concerns animating this case. For example, Chiu believed that Apple itself was collecting the UDID information at issue and testified that if he was mistaken—as he is—he would not have filed suit. Chiu Dep. 130:24–131:8. Nor does Chiu consider UDID to be “personal information.” *Id.* at 107:9–18. Ms. Capiro testified that she has *no* idea what information is transmitted to Apple when Location Services is on or off, and she never turned off Location Services for privacy. *Supra* p. 111; *see, e.g., Bodner v. Oreck Direct, LLC*, No. C 06-4756 MHP, 2007 WL 1223777, at \*2 (N.D. Cal. Apr. 25, 2007) (denying certification for lack of

1 typicality given “plaintiff’s undeniable and overwhelming ignorance regarding the nature of this  
2 action, the facts alleged, and the theories of relief against defendant”).

3 Moreover, Plaintiffs continue to engage in the very conduct they challenge, belying any claim  
4 that they face an imminent threat of harm; they lack incentives to pursue injunctive relief on behalf of  
5 the class, mooted their crucial function as class representatives. *Jordan v. Cnty. of Los Angeles*, 669  
6 F. 2d 1311, 1321 (9th Cir. 1982), *vac. on other grounds*, 459 U.S. 810 (1982).

## 7 **B. Plaintiffs Have Not Satisfied, and Cannot Satisfy, the Commonality Requirement**

### 8 **1. Plaintiffs Do Not Meet Their Burden of Demonstrating Common Evidence**

9 The Supreme Court’s *Dukes* decision “represents a significant restatement of [the Rule  
10 23(a)(2)] commonality requirement.” *Walter v. Hughes Commcn’s, Inc.*, No. 09-2136 SC, 2011 WL  
11 2650711, at \*7 (N.D. Cal. July 6, 2011). Following *Dukes*, “the raising of common questions—even  
12 in droves” is not enough to establish commonality. *Dukes*, 131 S. Ct. at 2551 (quotations omitted).  
13 Rather, *Dukes* makes clear that Plaintiffs must prove the existence not just of common questions  
14 (which “[a]ny competently crafted class complaint” can do), but of common evidence that is capable  
15 of generating “common *answers* apt to drive the resolution of the litigation.” *Id.*

16 Plaintiffs ignore their obligation to “affirmatively demonstrate” through convincing proof that  
17 there are “*in fact* . . . common questions of law or fact.” *Id.* And they make no attempt to identify  
18 what “common answers” could “resolve an issue that is central to the validity of each one of the  
19 claims in one stroke.” *Id.* Indeed, they fail to address the legal elements that would be required to  
20 prove their UCL and CLRA claims, much less prove that key elements could be resolved through  
21 common evidence for hundreds of millions of iDevice owners. *Compare Quesada v. Banc of Am.*  
22 *Inv. Servs., Inc.*, 11-CV-01703 YGR, 2013 WL 623288, at \*7 (N.D. Cal. Feb. 19, 2013).

### 23 **2. Plaintiffs’ UCL “Fraud” Claims Are Highly Individualized**

24 To establish a UCL fraud violation, Plaintiffs must identify a misrepresentation and produce  
25 “evidence showing ‘a likelihood of confounding an appreciable number of reasonably prudent  
26 purchasers exercising ordinary care.’” *Clemens v. DaimlerChrysler Corp.*, 534 F.3d 1017, 1026 (9th  
27 Cir. 2008). Plaintiffs cite three categories of representations that they apparently contend violate the  
28 UCL “fraud” prong (although they do not explain how). But they do not cite evidence that Apple

1 violated these provisions as to the named Plaintiffs, much less cite common evidence that these  
2 provisions could be deemed misleading to an “appreciable number” of Apple’s mobile users.

3 **a. Location Services Provisions: SLA and Device Setting**

4 Plaintiffs assert that Apple violated an SLA provision advising users that they could withdraw  
5 consent to have Apple collect, process, or transmit “your location data” by turning off Location  
6 Services. But Plaintiffs cannot show that a *single* user’s location data was ever collected by or  
7 transmitted to Apple (or anyone) while Location Services was off. *Supra* pp. 120–11. Likewise,  
8 Plaintiffs do not—and cannot—cite a single instance of iOS allowing an app to “determine [their]  
9 location” when Location Services was off.<sup>11</sup> Thus, no evidence exists to resolve the question of  
10 whether “[users’] location data” was transmitted to Apple, or whether the Location Services setting  
11 was “violated”—much less in a “single stroke” for every iOS user who turned Location Services off.

12 Nor would it be possible to prove that *any* data was transmitted to Apple’s servers for every  
13 iOS user who turned Location Services off. The iOS 4 bug was triggered only in *highly fact-specific*  
14 *settings*, depending on user behavior on the device and surrounding geography. *Supra* p. 12. Indeed,  
15 for the vast majority of users who turned Location Services off, no data (even the list of identifiers for  
16 publicly-broadcasting routers and cell towers in range) would or could have been sent to Apple.

17 **b. Privacy Policy Definition of UDID as “Non-Personal Information”**

18 Plaintiffs have abandoned their previous fraud claim and now point to a different provision in  
19 the Privacy Policy in arguing that Apple has “misidentif[ied]” UDID as “non-personal information.”  
20 Br. 9. As a threshold matter, Apple’s Privacy Policy applies to *Apple’s* own collection, use, and  
21 disclosure of user data, which expressly defines “personal information” as “data that can be used to  
22 uniquely identify or contact a single person,” and clearly categorizes data that cannot identify a  
23 person—like UDID—as “non-personal information.” Horvath Decl. ¶ 13. It further provides that  
24 when *Apple* combines personal and non-personal information, “the combined information will be  
25 treated as personal information *for as long as it remains combined.*” *Id.*

26 <sup>11</sup> Dr. Tribble’s Congressional testimony (delivered *after* the bug was resolved by iOS 4.3.3) cannot  
27 form the basis for classwide liability under the UCL, as it is not a “uniform” class-wide  
28 representation or “extensive and long-term” advertising campaign. There is no evidence that any  
Plaintiff, or the entire class, would have been exposed to or relied on it. *Supra* p. 3; *see, e.g.,*  
*Mazza*, 666 F.3d 581 at 595.

Again, Plaintiffs cite no evidence that these definitions are “false” or “misidentified” for any named Plaintiff, much less for all iOS device owners. Indeed, none of the Plaintiffs can show that any UDID could be used to identify or contact them, or that it was combined with other personal information. *Supra* pp. 5, 18. And Plaintiffs’ own experts admitted that UDID cannot be used to uniquely identify or contact an individual and have not identified a single instance of any app combining and transmitting UDID with personal information. *Id.* This failure eliminates any possibility of finding that these definitions were “false” as to an “appreciable number” of users.

Indeed, no such evidence exists, because the question of whether UDID could be used to identify or contact a specific individual requires a fact-specific inquiry: the possibility of linking UDID to an identifiable user fully depends on how the user used the device; what apps were downloaded; the practices of specific developers or third parties; what data a user provided to an app; and other individualized analyses wholly inconsistent with class treatment. *See Egele Dep.* 198:11–17; 208:3–20, 212:1–9; *see also Ellis* at 983 (requiring a “common pattern and practice that could affect that class as a whole”).

### c. SSL Encryption Claim

Plaintiffs also make no attempt to offer common evidence that could resolve their assertion that Apple’s statement regarding SSL encryption on its web pages is misleading, much less to every iOS device owner. *See supra* pp. 6, 18. Plaintiffs rely on a single transmission from the Pandora App to iTunes from Plaintiff Chiu’s device, *which they have no evidence was sent unencrypted.* *Supra* p. 6. Moreover, Plaintiffs found no comparable evidence of this supposed practice when performing the exact same tests on other Plaintiffs’ devices, each of which also had Pandora installed. Marziale Decl. ¶¶ 13–15. This stray, misguided example hardly suffices to show that Apple’s claims about SSL encryption on its webpage are “false” at all, much less on a classwide basis.

### 3. Plaintiffs’ UCL “Unfairness” Claims Are Highly Individualized

Plaintiffs’ remaining claims consist of generalized critiques of Apple’s internal policies and iOS technology, specifically: (i) Apple’s supposed “uneven enforcement” of its app review guidelines, particularly as to UDID; and (ii) allegedly excessive resource consumption on iOS

1 devices generally. Br. 11–12, 14–15. Plaintiffs apparently contend these practices are “unfair”<sup>12</sup>  
 2 under the UCL, since they make no attempt to tie them to any consumer-facing representation.  
 3 Plaintiffs supply no evidence to support the UCL “unfairness” requirements, however, which require  
 4 a court to “weigh the utility of the defendant’s conduct against the *gravity of the harm to the alleged*  
 5 *victim*”—an inquiry that is inherently individualized. *S. Bay Chevrolet v. GMAC*, 72 Cal. App. 4th  
 6 861, 886-87 (1999) (emphasis added); *see also Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152,  
 7 1169 (9th Cir. 2012). Here, *even the named Plaintiffs* cannot demonstrate unfairness, readily  
 8 conceding (i) they experienced no harm; and (ii) the benefits they obtained from using apps and  
 9 Location Services outweigh any hypothetical concerns. *Supra* p. 4. Moreover, these claims are  
 10 directed to highly variable practices and issues and intensively fact-specific contexts. Courts reject  
 11 class treatment of UCL unfairness claims when, as here, allegations are directed to a variable  
 12 business practice rather than a uniform policy. *Kaldenbach v. Mut. of Omaha Life Ins. Co.*, 178 Cal.  
 13 App. 4th 830, 850 (2009) (upholding denial of certification where “determination of what business  
 14 practices were allegedly unfair turns on individual issues”).

15 **a. Supposed “Uneven Enforcement” Of App Review Guidelines**

16 Plaintiffs’ core criticism of Apple’s app review practices—that Apple “selective[ly] enforces”  
 17 its PLA and App Store Review Guidelines and engages in “uneven” review of third-party apps—  
 18 defeats the required “showing of uniform conduct likely to mislead the entire class.” *Id.* The handful  
 19 of emails Plaintiffs cite only confirm that app review is a *highly individualized, fact-intensive process*  
 20 that varies by app and turns on the judgment, experience, and resource constraints of dozens of app  
 21 reviewers. This patchwork evidence underscores the lack of a uniform policy and the impossibility  
 22 of assessing whether Apple’s app review practices were “unfair” in “one stroke.” *See supra* pp. 6–8.

23 And Plaintiffs make no attempt to show how this supposedly “uneven” enforcement harmed  
 24 anyone or to cite common evidence that would permit a fact finder to weigh the utility of Apple’s

25  
 26 <sup>12</sup> Because the PLA and App Store Review Guidelines are only distributed to registered developers  
 27 and not distributed publicly, they cannot support a UCL “fraud” claim. TAC ¶ 78; Shoemaker  
 28 Decl. ¶¶ 7–10; *see, e.g., Mazza*, 666 F.3d at 595 (vacating class certification in part because “it  
 [was] likely that many class members were never exposed to the allegedly misleading  
 advertisements”); *In re Actimmune Mktg. Litig.*, No. C 08-02376-MHP, 2009 WL 3740648, at  
 \*11 (N.D. Cal. Nov. 6, 2009).

voluntary app review program against the hypothetical, individualized theories of harm Plaintiffs assert here. *Menagerie Prods. v. Citysearch*, No. CV 08-4263 CAS, 2009 U.S. Dist. LEXIS 108768, at \*48 (C.D. Cal. Nov. 9, 2009) (declining to certify a class because assessing “unfairness” would require an evaluation of *each class member’s* “individual expectations about the business practice”).

**b. Resource Consumption As A Result of “Unauthorized Transmissions” Depends on Myriad Factors**

Likewise, whether (and to what extent) a putative class member experienced “excessive” resource consumption due to “unauthorized” data transmissions implicates highly individualized, complex inquiries. Plaintiffs make the barest of arguments, conduct no analysis or investigation, and present no evidence that any one of them was impacted by this issue, as doing so would reveal the impossibility of replicating this exercise across millions of users. Of course, this inquiry cannot be answered with common proof; it is inherently device- and user-specific. Kravitz Decl., Ex. 7 (Egele Decl.) ¶¶ 91, 93, 97; Egele. Dep. 189:6–9. Indeed, all of the Plaintiffs concede that they did not experience any harm as a result of any resource depletion on their devices. *See supra* p. 4. There is no basis for presuming (or weighing) “harm” for millions of proposed class members.

In fact, all evidence shows that most members of the class derive far greater value from apps and location-based features than may be lost due to indiscernible resource consumption. Dwyer Dep. 139:5–141:12 (“happy” to provide apps with information like location); Chiu Dep. 100:6–21 (saying advertising is an acceptable cost of receiving free music); I. Capiro Dep. 46:24–47:14; 77:3–89:19 (provides location data so apps can “better locate and give directions”). Where, as here, individual class members would have different preferences and tolerances with respect to the challenged practice, class treatment of “unfairness” claims is inappropriate.<sup>13</sup>

**4. Plaintiffs’ CLRA Claims Require Individualized Determinations of Damage and Reliance That Preclude Commonality**

In addition to the above deficiencies, Plaintiffs’ inability to furnish common (or any) evidence that class members were damaged also prevents certification of their CLRA claims. “[I]t is well settled that to obtain relief under the CLRA, both the named plaintiff and unnamed class members

<sup>13</sup> If anything, the challenged practices may have conserved resources for certain users. Huang Decl. ¶ 31; *see Campion v. Old Republic Home Prot. Co., Inc.*, 272 F.R.D. 517, 533 (S.D. Cal. 2011) (determining class members’ harm “require[d] review of the particular circumstances).



1 must have suffered some damage caused by a practice deemed unlawful under [the CLRA].” *Sevidal*  
 2 *v. Target Corp.*, 189 Cal. App. 4th 905, 929 (2010) (quotations omitted); *Meyer v. Sprint Spectrum*  
 3 *L.P.*, 45 Cal. 4th 634, 644 (2009). Here, Plaintiffs concede they have not been damaged, and it thus  
 4 would be inappropriate to infer damages on behalf of the sweeping proposed class. *Supra* p. 4;  
 5 *Chamberlan v. Ford Motor Co.*, 369 F. Supp. 2d 1138, 1145 (N.D. Cal. 2005) (“[CLRA] relief . . . is  
 6 specifically limited to those who suffer damage, making causation a necessary element of proof”).

7 Likewise, determining causation here would require individualized determinations because a  
 8 classwide inference of reliance is not justified. Under the CLRA, “[c]ausation, on a class-wide basis,  
 9 may be established by materiality.” *In re Vioxx Class Cases*, 180 Cal. App. 4th 116, 129 (2009). But  
 10 where, as here, “materiality or reliance is a matter that would vary from consumer to consumer, the  
 11 issue is not subject to common proof, and the action is properly not certified as a class action.” *Id.*  
 12 As discussed (*supra* p. 3), *not one of the named Plaintiffs relied on any representation or deemed any*  
 13 *of the allegedly omitted information to be “material”*—indeed, they continued to use apps and  
 14 location features and to purchase iPhones even after filing their claims. But even if they had,  
 15 “materiality” would vary based on each user’s subjective experiences and views on privacy. *See*  
 16 *Webb v. Carter’s Inc.*, 272 F.R.D. 489, 502-03 (C.D. Cal. 2011) (CLRA claim not subject to common  
 17 proof where “consumers’ behavior would vary” even if they “saw the disclosure”; they “would not be  
 18 expected to respond uniformly to the message”); *Stearns v. Ticketmaster Corp.*, 655 F.3d 1013, 1045  
 19 (9th Cir. 2011) (denial of class certification affirmed where “proposed . . . class was so broad that it  
 20 cannot be said that the websites were ‘materially deficient’ as to the entire class”; “all of those people  
 21 [not misled] would [be] swept willy-nilly into the class”); *Caro v. Procter & Gamble Co.*, 18 Cal.  
 22 App. 4th 644, 668-69 (1993) (class treatment inappropriate as purchases were based on “personal  
 23 assumptions about the nature of the products”).

#### 24 **C. Plaintiffs Have Not Satisfied, and Cannot Satisfy, the Adequacy Requirement**

25 Plaintiffs also cannot satisfy Rule 23(a)(4). First, their claims are subject to myriad unique  
 26 defenses, including lack of standing and failure to establish any element of their claims. *See Deitz v.*  
 27 *Comcast Corp.*, No. C 06-06352 WHA, 2007 WL 2015440, at \*5 (N.D. Cal. Jul. 11, 2007) (denying  
 28 class certification where plaintiff “admitted that he had not read or relied on any of [defendant’s]

communications” and would be subject to unique defenses). Second, as Plaintiffs still voluntarily engage in the challenged practices and have updated their iOS software, they lack any incentive to “prosecute the action vigorously on behalf of the class.” *Ellis*, 657 F.3d at 985.

Finally, Plaintiffs seek injunctive relief that would be harmful to millions of class members who routinely download and benefit from free apps and use Location Services. “A class cannot be certified if class members benefit from the same acts alleged [by named plaintiffs] to be harmful to other members of the class.” *Pecover v. Elec. Arts Inc.*, No. C 08-2820 VRW, 2010 WL 8742757, at \*9 (N.D. Cal. Dec. 21, 2010) (quotations omitted). Plaintiffs admit they benefit from use of free apps and Location Services—and continue to use these features without concern for the purported data transmissions. *See Allied Orthopedic Appliances, Inc. v. Tyco Healthcare Grp. L.P.*, 247 F.R.D. 156, 177 (C.D. Cal. 2007) (“[N]o circuit approves of class certification where some class members derive a net economic benefit from the very same conduct alleged to be wrongful by the named representatives of the class, let alone where some *named* plaintiffs derive such a benefit.”).

#### VIII. THE PUTATIVE CLASSES CANNOT BE CERTIFIED UNDER RULE 23(B)(2)

Plaintiffs also do not come close to satisfying the requirements for certifying an injunctive relief class under Rule 23(b)(2), which is available only where “the party opposing the class has acted or refused to act *on grounds that apply generally to the class*, so that final injunctive relief or corresponding declaratory relief is appropriate *respecting the class as a whole*.” Fed. R. Civ. P. 23(b)(2) (emphasis added). Most fundamentally, Plaintiffs cannot make the essential showing that they—or anyone else—are “immediately in danger of sustaining some direct injury” or would benefit from the proposed relief. *See Los Angeles v. Lyons*, 461 U.S. at 102. Indeed, Apple has fully addressed Plaintiffs’ concerns in iOS updates that remove all app access to UDID and fix the limited iOS 4 bug, rendering their claims and proposed relief entirely moot. *Supra* p. 9. Finally, Plaintiffs’ jumble of proposed “remedies” would not benefit most iOS device owners and hardly present the type of categorical equitable relief appropriate for (b)(2) certification.

##### A. Plaintiffs Fail to Cite Any Ongoing or Imminent Harm That Could Be Redressed

Plaintiffs’ class claims do not establish the “real and immediate threat of repeated injury” required to obtain injunctive relief. *O’Shea*, 414 U.S. at 496; *see also In re Flash Memory Antitrust*



*Litig.*, No. C 07-0086 SBA, 2010 WL 2332081, at \*6 (N.D. Cal. June 9, 2010). Plaintiffs’ proposed relief includes revising Apple’s Privacy Policy to address UDID use by apps and enjoining Apple from “selective[] enforce[ment]” of its developer requirements related to UDID. Br. 10, 12. Yet these claims and proposed remedies are moot given Apple’s release of iOS 7, which removes all ability for apps to access UDID and other persistent identifiers. Neuenschwander Decl. ¶¶ 26–29. Further, Apple began rejecting all apps that requested UDID months ago as part of a long-planned transition away from UDID to new, non-persistent identifiers. *See id.* ¶ 24; Shoemaker Decl. ¶¶ 39–40. And since iOS 6, apps cannot access users’ personal information without a user’s express, on-device consent. Neuenschwander Decl. ¶ 25. In light of Apple’s voluntary changes, there is no “continuing” or “future injury” that Apple could remedy. *In re New Motor Vehicles Canadian Export Antitrust Litig.*, 522 F.3d 6, 14–16 (1st Cir. 2008).

Likewise, Plaintiffs broadly propose that the Court enjoin “the ongoing conduct by which iDevices continue to use Location Services [when off],” and enjoin “Apple from collecting or storing location-based information [once Location Services is off].” Br. 19. But years ago, Apple provided—and Plaintiffs downloaded—iOS updates that fully remedied the geolocation bug by

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**B. The Proposed Relief Would Not Benefit the Class as a Whole—or Even Most of It**

Plaintiffs propose to dictate a host of misguided and impossible business changes that are either moot or would have widely disparate and negative consequences for users, none of which represent “appropriate” “declaratory relief . . . *respecting the class as a whole.*” Fed. R. Civ. P. 23(b)(2) (emphasis added). As one example, Plaintiffs propose a series of changes to Apple’s UDID policies based on the claim that certain “legacy devices” will continue to allow access to UDID

[REDACTED]

[REDACTED]

1 [REDACTED]  
 2 Separately, Plaintiffs vaguely propose to enjoin Apple from “selectively enforcing” the PLA  
 3 and App Review Guidelines. Br. 12. [REDACTED]  
 4 [REDACTED]  
 5 [REDACTED]  
 6 [REDACTED]  
 7 [REDACTED]

8 Plaintiffs also propose to enjoin Apple from “collecting or storing location-based  
 9 information” when Location Services is turned off, but as discussed, this proposal is moot for most of  
 10 the class members who have upgraded to iOS 4.3.3 or later. And because Apple cannot update or  
 11 delete the iOS software already on users’ devices (Neuenschwander Decl. ¶ 31), no software update  
 12 could possibly “provide relief to *each* member of the class.” *Schulken*, 2012 WL 28099, at \*6.

13 Finally, Plaintiffs’ argument that Rule 23(b)(2) certification is appropriate “even where only a  
 14 subset of the Class has been affected by the conduct at issue,” or where “class representatives are the  
 15 only members who actually suffered an alleged injury,” directly contradicts controlling authority. Br.  
 16 6; *see Dukes*, 131 S. Ct. at 2558 (a 23(b)(2) class must request “an indivisible injunction benefitting  
 17 all its members at once”); *Cholakyan*, 281 F.R.D. at 559.<sup>14</sup>

#### 18 **IX. THE PUTATIVE “LIABILITY-ONLY” CLASS (“BATTERY LIFE/BANDWIDTH** 19 **CLASS”) CANNOT BE CERTIFIED UNDER RULE 23(B)(3)**

20 Plaintiffs also propose—for the first time—a Rule 23(b)(3) “liability-only” class purportedly  
 21 “consisting of iDevice owners who, as a result of Apple’s geo-tagging activities in [alleged] violation  
 22 of the CLRA or (ii) Apple’s [alleged] misrepresentations and omissions regarding unauthorized  
 23 transmissions of user data, experienced shortened battery life and increased bandwidth usage.” Br.  
 24 24. This proposed class fails on every basis: It was not pled by Plaintiffs, none of the Plaintiffs has  
 25 standing to represent it, and Plaintiffs cannot meet the requirements of Rule 23(a).

26 <sup>14</sup> Unsurprisingly, the cases Plaintiffs cite in support of this assertion provide only that class  
 27 members need not be affected *in the same way*—not that they need not be affected *at all*. *See*  
 28 *Burdick v. Union Sec. Ins. Co.*, No. CV 07-4028 ABC (JCX), 2009 WL 6541608, at \*16 (C.D.  
 Cal. April 2, 2009); *Arnold v. United Artists Theatre Circuit, Inc.*, 158 F.R.D. 439, 448 (N.D. Cal.  
 1994) (defendants’ conduct “need not affect each member of the class *in the same manner*”).

Moreover, this proposed class fails to satisfy Rule 23(b)(3)'s requirements that common questions predominate over individual issues.<sup>15</sup> *See Wang*, 709 F.3d at 835; *see also Comcast*, 133 S. Ct. at 1432. Indeed, determining whether each consumer “experienced shortened battery life and increased bandwidth usage” specifically as a result of geo-tagging or unauthorized data transmissions requires dozens of individualized inquiries. *Supra* p. 16. Because these individualized issues predominate, Plaintiffs fail to meet this requirement. *See Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1188–90 (9th Cir. 2001); *In re Wells Fargo Home Mortg. Overtime Pay Litig.*, 571 F.3d 953, 959 (9th Cir. 2009); *Wash. v. Joe’s Crab Shack*, 271 F.R.D. 629, 638 (N.D. Cal. 2010).

Plaintiffs also admit that “a unitary theory of damage to each and every class member cannot be stated with any particularity as to the class as a whole.” Br. 26. This, too, is fatal to their proposed class. *See Comcast*, 133 S. Ct. at 1433 (plaintiffs’ failure to distinguish and link each liability theory and damages assessment rendered predominance prerequisite a “nullity”); *Guido v. L’Oreal, USA, Inc.*, No. CV 11-1067 CAS JCX, 2013 WL 3353857, at \*15 (C.D. Cal. July 1, 2013) (23(b)(3) class only suitable with “evidence” showing “classwide method of awarding relief” “consistent with the plaintiffs’ theory of liability”). Simply adding the prefix “liability-only” to the proposed class makes no difference: Plaintiffs still must establish predominance.<sup>16</sup>

Finally, Plaintiffs fail to show that any class proceeding would be manageable or superior. *See Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 607 (1997). They present no classwide proof, methodology, or trial plan, as any class would be wholly unmanageable. *See Fed. R. Civ. P. 23*, Adv. Comm. Notes (“party requesting class certification [should] present a ‘trial plan’ that describes the issues likely to be presented at trial and tests whether they are susceptible of class-wide proof”).

## X. CONCLUSION

For the above reasons, Plaintiffs’ Motion for Class Certification should be denied.

<sup>15</sup> They fail to meet this test even under the cases they cite. *See, e.g., In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig.*, 722 F.3d 838, 860 (6th Cir. 2013) (“[L]iability . . . relating to injury must be susceptible of proof on a classwide basis to meet the predominance standard”).

<sup>16</sup> Plaintiffs’ citations regarding Rule 23(b)(3) certification are inapposite; nowhere in *Ellis v. Costco Wholesale Corp. (II)*, 285 F.R.D. 492, 539 (N.D. Cal. 2012) or *Munoz v. PHH Corp.*, No. 1:08-CV-0759-AWI-BAM, 2013 WL 2146925 (E.D. Cal. May 15, 2013) did the court indicate that plaintiffs could avoid the predominance requirement by certifying a liability-only 23(b)(3) class.

1 Dated: September 19, 2013

Respectfully submitted,

2 GIBSON, DUNN & CRUTCHER LLP

3  
4 By: S. Ashlie Beringer  
S. Ashlie Beringer

5 Attorneys for Defendant  
6 APPLE INC.

# APPENDIX A

## APPENDIX A

### Summary of Forensic Analysis of Plaintiffs' Claims

Plaintiff	Specified App	Alleged Data Collected Available Through Apple API	Alleged Data Collected Available Only From Plaintiff or App	Third-Party Companies That Allegedly Received Data	Evidentiary Support?
Chiu <i>TAC ¶ 40(c)</i>	Dictionary.com	UDID		Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 38.</i>
Chiu <i>TAC ¶ 40(c)</i>	Dictionary.com	Device type and model		Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 38.</i>
Chiu <i>TAC ¶ 40(c)</i>	Dictionary.com	Name of operating system and version		Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 38.</i>
Chiu <i>TAC ¶ 40(c)</i>	Dictionary.com	Time zone		Flurry	Yes. <i>Bolas Decl. ¶ 38.</i>
Chiu <i>TAC ¶ 40(a)</i>	Dictionary.com		Titles of particular pages in the App plaintiff viewed	Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 48.</i>
Chiu <i>TAC ¶ 40(a)</i>	Dictionary.com		Particular app activities plaintiff used	Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 48.</i>
Chiu <i>TAC ¶ 40(c)</i>	Dictionary.com	Language		Flurry	Yes. <i>Bolas Decl. ¶ 38.</i>
Chiu <i>TAC ¶ 41(a)</i>	Dictionary.com	UDID		AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 37.</i>

Plaintiff	Specified App	Alleged Data Collected Available Through Apple API	Alleged Data Collected Available Only From Plaintiff or App	Third-Party Companies That Allegedly Received Data	Evidentiary Support?
Chiu <i>TAC</i> ¶ 41(a)	Dictionary.com	Network type		AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 37.</i>
Chiu <i>TAC</i> ¶ 41(a)	Dictionary.com	Name of device's operating system and version		AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 37.</i>
Chiu <i>TAC</i> ¶ 41(a)	Dictionary.com	"Carrier-assigned username" [device name]		AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 37.</i>
Chiu <i>TAC</i> ¶ 43(a)	Dictionary.com		Search terms entered	Google Analytics	<b>No support.</b> <i>Bolas Decl. ¶ 49.</i>
Chiu <i>TAC</i> ¶ 40(c)	Urban Spoon	UDID		Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 45.</i>
Chiu <i>TAC</i> ¶ 40(c)	Urban Spoon	Device type and model		Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 43.</i>
Chiu <i>TAC</i> ¶ 40(c)	Urban Spoon	Name of operating system and version		Flurry	<b>No support.</b> <i>Bolas Decl. ¶ 43.</i>
Chiu <i>TAC</i> ¶ 40(c)	Urban Spoon	Time zone		Flurry	Yes. <i>Bolas Decl. ¶ 44.</i>
Chiu <i>TAC</i> ¶ 40(b)	Urban Spoon		Titles of particular pages in the App plaintiff viewed	Flurry	Yes. <i>Bolas Decl. ¶ 59.</i>

Plaintiff	Specified App	Alleged Data Collected Available Through Apple API	Alleged Data Collected Available Only From Plaintiff or App	Third-Party Companies That Allegedly Received Data	Evidentiary Support?
Chiu <i>TAC ¶ 40(b)</i>	Urban Spoon		Particular app activities plaintiff used	Flurry	Yes. <i>Bolas Decl. ¶ 59.</i>
Chiu <i>TAC ¶ 40(c)</i>	Urban Spoon	Language		Flurry	Yes. <i>Bolas Decl. ¶ 44.</i>
Chiu <i>TAC ¶ 42(e)</i>	Urban Spoon	UDID		DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 42.</i>
Chiu <i>TAC ¶ 42(e)</i>	Urban Spoon	Fine GPS-based location information		DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 42.</i>
Chiu <i>TAC ¶ 42(e)</i>	Urban Spoon		Type of search	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 58.</i>
Chiu <i>TAC ¶ 42(e)</i>	Urban Spoon		Food type	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 58.</i>
Chiu <i>TAC ¶ 41(b)</i>	Pandora		Unique non-Apple identifier	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 54.</i>
Chiu <i>TAC ¶ 41(c)</i>	Pandora		Date of birth	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 54.</i>
Chiu <i>TAC ¶ 41(c)</i>	Pandora		Gender	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 54.</i>
Chiu <i>TAC ¶ 41(c)</i>	Pandora		Income	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 54.</i>



Plaintiff	Specified App	Alleged Data Collected Available Through Apple API	Alleged Data Collected Available Only From Plaintiff or App	Third-Party Companies That Allegedly Received Data	Evidentiary Support?
Chiu <i>TAC ¶ 41(c)</i>	Pandora		Education level	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 54.</i>
Chiu <i>TAC ¶ 41(c)</i>	Pandora		Partners sought	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 54.</i>
Chiu <i>TAC ¶ 42(a)</i>	Pandora		Age	DoubleClick	Possible. <i>Bolas Decl. ¶ 57.</i>
Chiu <i>TAC ¶ 42(a)</i>	Pandora		Gender	DoubleClick	Possible. <i>Bolas Decl. ¶ 55.</i>
Chiu <i>TAC ¶ 42(a)</i>	Pandora		Zip Code	DoubleClick	Possible. <i>Bolas Decl. ¶ 57.</i>
Chiu <i>TAC ¶ 42(a)</i>	Pandora		Song and performer selected	DoubleClick	Possible. <i>Bolas Decl. ¶ 55.</i>
Chiu <i>TAC ¶ 42(a)</i>	Pandora		Music genre	DoubleClick	Possible. <i>Bolas Decl. ¶ 55.</i>
Chiu <i>TAC ¶ 42(a)</i>	Pandora		Link to identifier shared with AdMarvel	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 54.</i>
Chiu <i>TAC ¶ 43(b)</i>	Flixster	Operating system and version		Google Analytics	Yes. <i>Bolas Decl. ¶ 40.</i>
Chiu <i>TAC ¶ 43(b)</i>	Flixster		Movie requested	Google Analytics	Yes. <i>Bolas Decl. ¶ 52.</i>

Plaintiff	Specified App	Alleged Data Collected Available Through Apple API	Alleged Data Collected Available Only From Plaintiff or App	Third-Party Companies That Allegedly Received Data	Evidentiary Support?
Chiu <i>TAC ¶ 43(b)</i>	Flixster		Activity within app	Google Analytics	Yes. <i>Bolas Decl. ¶ 52.</i>
Chiu <i>TAC ¶ 43(b)</i>	Flixster		Pages viewed	Google Analytics	Yes. <i>Bolas Decl. ¶ 52.</i>
Chiu <i>TAC ¶ 42(c)</i>	Flixster	Device operating system		DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 39.</i>
Chiu <i>TAC ¶ 42(c)</i>	Flixster		Presence of SD card	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 51.</i>
Chiu <i>TAC ¶ 42(c)</i>	Flixster		Whether phone is jail-broken	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 50.</i>
Chiu <i>TAC ¶ 42(c)</i>	Flixster		Keywords for other data values	DoubleClick	Possible. <i>Bolas Decl. ¶ 53.</i>
Chiu <i>TAC ¶ 42(b)</i>	Flixster		Particular movie requested	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 50.</i>
Chiu <i>TAC ¶ 42(b)</i>	Flixster		Genre	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 50.</i>
Chiu <i>TAC ¶ 42(b)</i>	Flixster		Whether a “Certified Fresh” review was available	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 50.</i>

Plaintiff	Specified App	Alleged Data Collected Available Through Apple API	Alleged Data Collected Available Only From Plaintiff or App	Third-Party Companies That Allegedly Received Data	Evidentiary Support?
Chiu <i>TAC ¶ 42(d)</i>	Weather Channel	Model		DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 46.</i>
Chiu <i>TAC ¶ 42(d)</i>	Weather Channel		Zip Code	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 60.</i>
Dwyer <i>TAC ¶ 41(b)</i>	Pandora		Non-Apple unique identifier “downloaded from DoubleClick”	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 68.</i>
Dwyer <i>TAC ¶ 41(c)</i>	Pandora		Date of birth	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 71.</i>
Dwyer <i>TAC ¶ 41(c)</i>	Pandora		Gender	AdMarvel	Possible. <i>Bolas Decl. ¶ 71.</i>
Dwyer <i>TAC ¶ 41(c)</i>	Pandora		Income	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 71.</i>
Dwyer <i>TAC ¶ 41(c)</i>	Pandora		Education level	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 71.</i>
Dwyer <i>TAC ¶ 41(c)</i>	Pandora		Partners sought	AdMarvel	<b>No support.</b> <i>Bolas Decl. ¶ 71.</i>
Dwyer <i>TAC ¶ 42(a)</i>	Pandora		Age	DoubleClick	Possible. <i>Bolas Decl. ¶ 69.</i>

Plaintiff	Specified App	Alleged Data Collected Available Through Apple API	Alleged Data Collected Available Only From Plaintiff or App	Third-Party Companies That Allegedly Received Data	Evidentiary Support?
Dwyer <i>TAC ¶ 42(a)</i>	Pandora		Gender	DoubleClick	Possible. <i>Bolas Decl. ¶ 69.</i>
Dwyer <i>TAC ¶ 42(a)</i>	Pandora		Zip Code	DoubleClick	Possible. <i>Bolas Decl. ¶ 69.</i>
Dwyer <i>TAC ¶ 42(a)</i>	Pandora		Song and performer selected	DoubleClick	Possible. <i>Bolas Decl. ¶ 69.</i>
Dwyer <i>TAC ¶ 42(a)</i>	Pandora		Music genre	DoubleClick	Possible. <i>Bolas Decl. ¶ 69.</i>
Dwyer <i>TAC ¶ 42(a)</i>	Pandora		Link to identifier shared with AdMarvel	DoubleClick	<b>No support.</b> <i>Bolas Decl. ¶ 68.</i>